

DOCUMENT-IDENTIFIER: JP 63039228 A

Page 1 of 1

PAT-NO: JP363039228A

DOCUMENT-IDENTIFIER: JP 63039228 A

TITLE: SECRET SECURING SYSTEM

PUBN-DATE: February 19, 1988

Best Available Copy

INVENTOR-INFORMATION:

NAME **COUNTRY**

TACHIBANA, NORIYUKI

ASSIGNEE-INFORMATION:

NAME **COUNTRY**

NEC CORP N/A

APPL-NO: JP61183602

APPL-DATE: August 4, 1986

INT-CL (IPC): H04L009/00

ABSTRACT:

PURPOSE: To further improve capability to secure secret by adding the interval of inputting a password as password information and checking the password and said interval.

CONSTITUTION: The titled system includes a password information input part 100 and a password information verifying part 200. Before transmitting the inputted password, the input part 100 sets the reading of a timer to an input time interval. After the inputted digit is incremented since the password was transmitted, the part 100 is waiting until the set input time interval as the reading of the timer expires. The part 100 inputs and transmits the password of the next digit. These procedures are repeated until the last digit. The verifying part 200 receives and holds password information from the input part 100, and further holds the reception time. That is repeated by the number of the digits of the password. After the entire password is inputted, the reception input time interval is obtained from the reception time, and the received password is checked whether it agrees with a registered one. If so, the reception input time interval is checked whether it is included in a registered input time interval permissible range. If so, an access to secret securing information is permitted; otherwise, any access is inhibited.

COPYRIGHT: (C)1988,JPO&Japio

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

昭63-39228

⑤ Int.Cl.⁴

H 04 L 9/00

識別記号

庁内整理番号

A-7240-5K

④ 公開 昭和63年(1988)2月19日

審査請求 未請求 発明の数 1 (全4頁)

⑬ 発明の名称 機密保全システム

⑭ 特 願 昭61-183602

⑮ 出 願 昭61(1986)8月4日

⑯ 発 明 者 橋 則 行 東京都港区芝5丁目33番1号 日本電気株式会社内
⑰ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号
⑱ 代 理 人 弁理士 内 原 晋

明 細 書

1. 発明の名称

機密保全システム

2. 特許請求の範囲

機密保全システムにおいて、

投入された暗証番号を1桁毎に順次送信する暗証情報投入部と、

登録された暗証番号と、登録された暗証番号投入時間間隔と、登録された投入時間間隔許容範囲を予め保持しており、暗証情報入力部から受信した暗証番号と受信時刻を保持して、該暗証番号と登録暗証番号が一致し、かつ、前記受信時刻から算出された暗証番号投入時間間隔情報が、登録暗証番号投入時間間隔許容範囲の中に含まれる場合にのみ暗証情報確認正常とみなし、機密保全システムへのアクセスを許可する暗証情報検証部を備えたことを特徴とする機密保全システム。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は暗証番号を必要とする機密保全システ

ムに関する。

(従来の技術)

従来、この種の機密保護システムでは、入力された暗証番号と登録された暗証番号を順に比較し、一致したかどうかにより、暗証番号の確認を行っていた。

第4図は従来の機密保全システムの暗証番号確認方式を示すフローチャートである。

機密保全システムは暗証番号投入部と暗証番号検証部を含んでいる。

暗証番号投入部は、処理開始とともに、投入桁数を初期化する(ステップ1)。次に暗証番号が1桁投入されると、その暗証番号を暗証番号検証部に送信し(ステップ2)、投入桁数を+1インクリメントし(ステップ3)、投入桁数が暗証桁数より小さいか否かを判断し(ステップ4)、小さければステップ2に戻り、ステップ3、4を繰り返す。ステップ4で投入桁数が暗証桁数と等しければ暗証番号の投入処理は終了する。一方、暗証番号検証部は処理開始とともに、受信桁数を初

期化する(ステップ11)。次に暗証番号投入部から送信された暗証番号の1桁を受信する(ステップ12)と、その暗証番号を保持(ステップ13)し、受信桁数を+1インクリメントし(ステップ14)、受信桁数が暗証番号桁数より小さいか否かを判断し(ステップ15)、小さければステップ12に戻る。受信桁数が暗証番号桁数と一致すれば受信暗証番号と登録暗証番号とが一致するか否かを判断し(ステップ16)、一致している場合は機密保全システムへのアクセスが許可され、一致していない場合には該アクセスが禁止される。

(発明が解決しようとする問題点)

上述した従来の暗証情報確認方式は、入力される情報は暗証番号のみであるため、暗証番号入力手段としてコンピュータを使用して暗証番号の発生と暗証確認のチェックを自動化した場合など、暗証番号の桁数が十分多くなければ暗証番号を探し出すことができ、機密の防止ができないという欠点がある。

(問題点を解決するための手段)

実施例を示すフローチャート、第2図は機密保全システムの要部構成図である。

機密保全システムは暗証情報投入部100と暗証情報検証部200を含んでいる。本実施例の暗証情報投入部100は第4図の暗証番号投入部に暗証情報投入時間間隔を設定する処理5、7および時間待ち処理6が付加されたものである。また、暗証情報検証部200は、登録暗証番号、登録暗証番号投入時間間隔、登録投入時間間隔許容範囲を予め保持し、暗証情報投入部100から暗証番号を受信した時間を保持する処理16、受信時間から暗証番号投入時間間隔(以下投入時間間隔と記す)を算出する処理17、投入時間間隔と登録投入時間間隔の一致、不一致を判断するステップ18が第4図の暗証番号検証部に付加されたものである。

暗証情報投入部100は、投入された暗証番号を送信する(ステップ2)前にタイマー値を投入時間間隔に設定し(ステップ5または7)、暗証番号送信(ステップ2)後、投入桁数を+1インクリメントした(ステップ3)後、タイマー値とし

本発明の機密保全システムは、投入された暗証番号を1桁毎に順次送信する暗証情報投入部と、

登録された暗証番号と、登録された暗証番号投入時間間隔と、登録された投入時間間隔許容範囲を予め保持しており、暗証情報入力部から受信した暗証番号と受信時刻を保持して、該暗証番号と登録暗証番号が一致し、かつ、前記受信時刻から算出された暗証番号投入時間間隔情報が、登録暗証番号投入時間間隔許容範囲の中に含まれる場合にのみ情報確認正常とみなし、機密保全システムへのアクセスを許可する暗証情報検証部を備えたことを特徴とする。

このように、暗証情報として暗証番号投入時間間隔を付加して、暗証番号と暗証番号投入時間間隔の両者をチェックすることにより、機密保全能力を一層高めることができる。

(実施例)

次に、本発明の実施例を図面を参照して説明する。

第1図は本発明の機密保全システムの第1の実

て設定された投入時間間隔が経過するまで時間待ち(ステップ6)して次の桁の暗証番号を投入し送信する(ステップ2)。これを暗証桁数まで順次繰り返す。暗証情報検証部200は暗証番号投入部100からの暗証情報を受信保持し(ステップ12、13)、さらにその受信時間をも保持する(ステップ16)。これを暗証桁数だけくり返し行い、全ての暗証番号投入後、受信時間より受信投入時間間隔を求め(ステップ17)、受信暗証番号が登録暗証番号と一致しているかどうかをチェックし(ステップ18)、一致していれば受信投入時間間隔が登録投入時間間隔許容範囲に含まれているかチェックし(ステップ18)、許容範囲内であれば機密保全情報へアクセス許可し、それ以外はアクセス禁止する。

第3図は第2の実施例を示すフローチャートである。

前述の第1の実施例においては、暗証番号の1桁毎の投入時間間隔は、暗証情報投入部100で設定されている。したがって暗証番号の次の桁を投

入するまでの時間は時間待ち（ステップ6）として暗証情報投入部100のフローチャート中に含まれる。

しかし、例えば暗証番号投入手段が簡単な押ボタン式の機器で、人間が暗証している時間毎に1桁ずつ暗証番号を投入する場合、あるいはマイクロコンピュータに暗証番号と暗証投入時間間隔を設定し、それ以後はマイクロコンピュータが機械的に、暗証投入時間間隔毎に暗証番号を暗証情報投入部に入力する場合には、第1の実施例のステップ5、6、7に相当する時間処理は人間またはマイクロコンピュータ中で行われる。したがって、暗証情報投入部100の処理としては、ステップ5、6、7は不必要で、第4図の暗証番号投入部の処理と同様になる。その結果、第2の実施例においては、暗証情報投入部100は従来の暗証番号投入部と同様であり、暗証情報検証部200は第1図と同様である。なお、第1図、第3図には暗証番号の途中放棄などの検出タイミングなどの処理は記入されていない。また、受信間隔の算出

は、暗証番号受信のつど行っても良い。

（発明の効果）

以上説明したように本発明は、暗証情報として、暗証番号投入時間間隔を付加することにより、機械的に暗証情報を発生させて暗証確認チェックをさせる悪意者に対してシステムの機密保全能力を高めることができ、さらに、暗証番号の入力手段を機械的にさせるシステムでは、暗証番号投入時間間隔を精密な時間に設定可能であるため、時間間隔の情報量をかなり多くとることができる、暗証情報量が増えるので、機密保全能力を一段と高めることができる効果がある。

4. 図面の簡単な説明

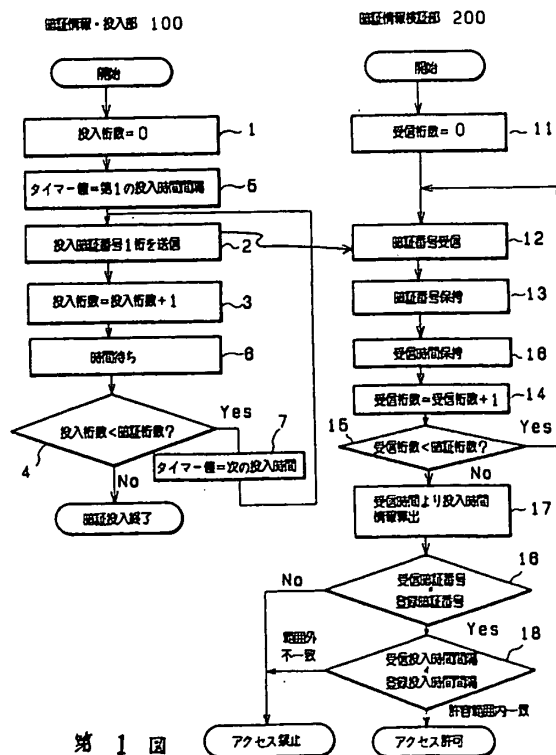
第1図は本発明の機密保全システムの第1の実施例を示すフローチャート、第2図は機密保全システムの構成図、第3図は本発明の機密保全システムの第2の実施例を示すフローチャート、第4図は機密保全システムの従来例のフローチャートである。

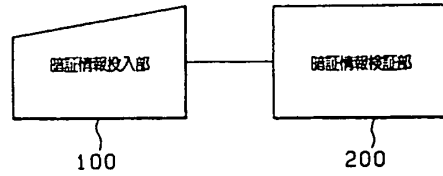
100 … 暗証情報投入部、

200 … 暗証情報検証部、

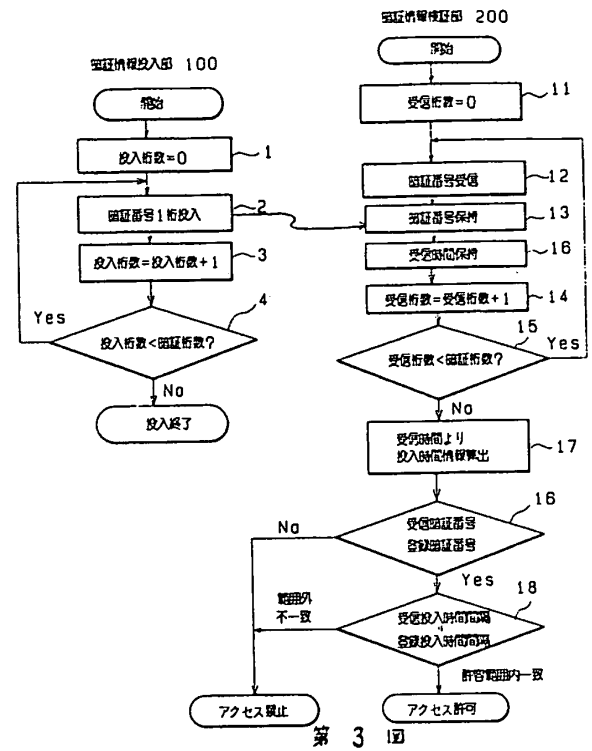
特許出願人 日本電気株式会社
代理人 弁理士 内原 晋

(弁理士 内原 晋)

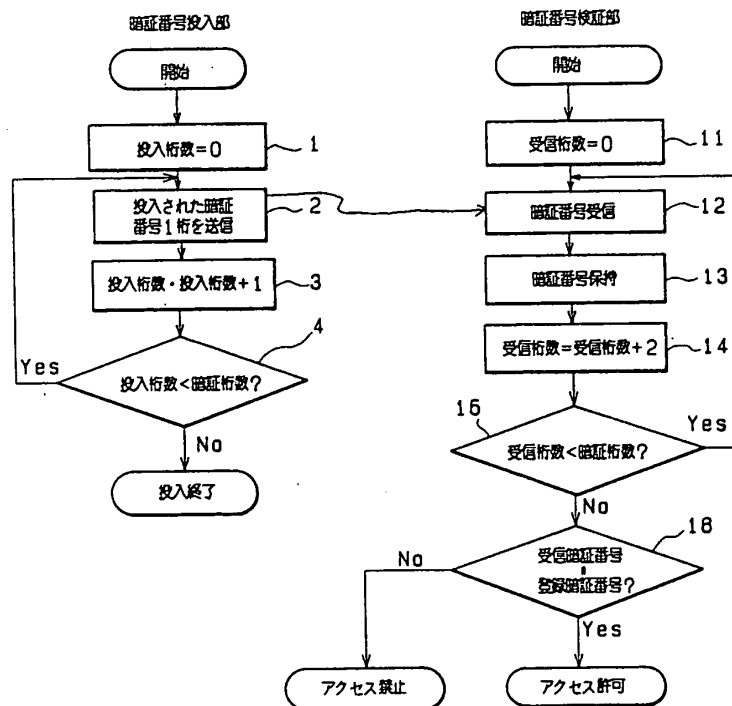




第 2 図



第 3 図



第 4 図

PAT-NO: JP363039228A

DOCUMENT-IDENTIFIER: JP 63039228 A

TITLE: SECRET SECURING SYSTEM

PUBN-DATE: February 19, 1988

INVENTOR-INFORMATION:

NAME

TACHIBANA, NORIYUKI

ASSIGNEE-INFORMATION:

NAME

NEC CORP

COUNTRY

N/A

APPL-NO: JP61183602

APPL-DATE: August 4, 1986

INT-CL (IPC): H04L009/00

ABSTRACT:

PURPOSE: To further improve capability to secure secret by adding the interval of inputting a password as password information and checking the password and said interval.

CONSTITUTION: The titled system includes a password information input part 100 and a password information verifying part 200. Before transmitting the inputted password, the input part 100 sets the reading of a timer to an input time interval. After the inputted digit is incremented since the password was transmitted, the part 100 is waiting until the set input time interval as the reading of the timer expires. The part 100 inputs and transmits the password of the next digit. These procedures are repeated until the last digit. The verifying part 200 receives and holds password information from the input part 100, and further holds the reception time. That is repeated by the number of the digits of the password. After the entire password is inputted, the reception input time interval is obtained from the reception time, and the received password is checked whether it agrees with a registered one. If so, the reception input time interval is checked whether it is included in a

registered input time interval permissible range. If so, an access to secret
securing information is permitted: otherwise, any access is inhibited.

COPYRIGHT: (C)1988,JPO&Japio

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.